

Access Policy

August 2012



ON CYBER PATROL



During our formative years we are taught by our parents, teachers and relatives how to be nice and how we should treat others. We are taught what we should and should not do, as well as what we should and should not say. Most young men are taught to hold the door for ladies, and offer assistance to people with their hands full. Even today some grocery stores offer to carry your bags to your car free of charge. Yes, we are always trying to be helpful. How many times have you said "let me get the door for you" or offered to hold the door for someone as they are entering an establishment at the same time? Whereas this learned quality may be the courteous thing to do, it is not always the right thing to do.

Many of us work in controlled access facilities that monitor entry and exit points. There are countless security protocols in place to help protect not only the information inside our offices, but also help protect the individuals working there as well. Security protocols require that everyone entering a facility verify their identity and authorization to access the facility every time they enter. But many times people try to circumvent these protocols by "piggybacking" off someone as that person is entering a facility. In security, piggybacking refers to when a person follows an authorized person into a restricted area without showing their own authorization to access the area. There are many reasons it is done and none of them are acceptable. The reasons for piggybacking include but are not limited to:

- Gaining access to a prohibited area
- Attempting to avoid sign-in delay
- Reluctance to retrieve credentials
- Forgot their credentials at home or in the office
- Others holding the door to be polite

Some instances of piggybacking can be attributed to laziness but there are many instances that the person you held the door for has no right to be in the facility. It does not require a lot of time or effort for a skilled individual with the proper social engineering skills to inflict damage on an organization. Once that person has gained access there are very few measures that would stop them from causing damage to IT systems and data systems. There is a great deal of information that can be gained by simply walking around and reading documents left on copy machines or unattended desks. There have been instances where an intruder used an internal phone to place calls to other office numbers telling the person there was someone downstairs to be escorted. Once that person who was called left their desk, the intruder rifled through their work area and even removed personal electronic devices. This example may not be the typical case of what can happen, but we must remain vigilant in our efforts to guard our interests. One of the first steps to ensuring we protect ourselves and our organization is to adhere to all security protocols addressing controlled access.

If they have two cups of coffee or have their hands full offer, to hold something while they retrieve their credentials...it's much better than explaining how you let the organization get illegally accessed!